AT&T breach involving 2022 customer data caused by third-party 'threat actor'

July 15 2024, by Andrew Long, The Dallas Morning News

Credit: Unsplash/CC0 Public Domain

Dallas-based telecommunications company AT&T revealed its second data breach of the year July 12, a leak that affects more than 100 million U.S. customers.

The cause of the breach was not a breakdown of company servers, the company said, but a malicious actor who illegally broke into an AT&T workspace from a remote platform.

According to Securities and Exchange Commission filings, AT&T first learned about the data breach on April 19 of this year after a "threat actor claimed to have unlawfully accessed and copied AT&T call logs."

This "threat actor" gradually siphoned the data from an AT&T workspace through a "third-party cloud platform" between April 14–25, during which time the company had begun an investigation into the breach with the help of external cybersecurity experts.

The data contains communication records from May 1 to Oct. 31, 2022, as well as on Jan. 2, 2023. The concerned data was not taken on those dates, but from those dates after the fact.

The company said that nearly all AT&T wireless customers and customers of mobile virtual network operators hosted by AT&T servers, like Cricket Wireless or StraightTalk, could be impacted. AT&T serves more than 100 million U.S. customers and a further 2.5 million businesses, the second-most behind Verizon.

AT&T said that the leaked data does not include any personal identification information like social security numbers, age or credit card information, nor does it contain the content of phone calls and texts.

Instead, it includes records of communications during the affected periods, including the other phone numbers a wireless number interacted with as well as call duration. AT&T said that all affected customers will be notified if their data was involved in the breach.

AT&T said that "while the data does not include customer names, there

are often ways, using publicly available online tools, to find the name associated with a specific telephone number."

The company also said that it does not believe the breached data is publicly available and that it does not believe the breach is "reasonably likely to materially impact AT&T's financial condition or results of operations."

The company's first data breach of the year occurred roughly a month before the larger breach was uncovered. Nearly 73 million current and former AT&T companies had social security numbers and names leaked onto the dark web, opening them up to potential identity fraud and other dangers.

Digital privacy is a growing issue and online users should be cautious of malicious parties looking to steal and use their data. Recommended personal protection measures include credit freezes, multi-factor account authentication and changing passwords to include more complete number-letter-symbol arrangements.

2024 The Dallas Morning News. Distributed by Tribune Content Agency, LLC.

Citation: AT&T breach involving 2022 customer data caused by third-party 'threat actor' (2024, July 15) retrieved 16 July 2024 from https://techxplore.com/news/2024-07-att-breach-involving-customer-party.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.